



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/016,558	12/06/2001	Albert Young	3COM-3730.CTO.US.P	6325

7590 03/29/2006

WAGNER, MURABITO & HAO LLP
Third Floor
Two North Market Street
San Jose, CA 95113

EXAMINER

SIMITOSKI, MICHAEL J

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 03/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/016,558

Applicant(s)

YOUNG ET AL.

Examiner

Michael J. Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 January 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-60 is/are pending in the application.
- 4a) Of the above claim(s) 2-7, 20, 22-27, 40, 42-47 and 60 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1, 8-19, 21, 28-39, 41 and 48-59 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 December 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The response of 1/23/2006 was received and considered.
2. Claims 1-60 are pending. Claims 1, 8-19, 21, 28-39, 41 & 48-59 are under consideration.

Response to Arguments

3. Applicant's response (p. 19) argues that See does not disclose authenticating a central authentication server to a client device nor does See disclose determining an authentication key at a client device or at the central authentication server. However, Applicant appears to be relying on the limitation "client device", which is open to broadest reasonable interpretation. See's authentication agent is acting on behalf of the client and therefore is a client device. Further, the network management system is an authentication server (Fig. 1). Therefore, it is maintained that See discloses authenticating a central authentication server to a client device. Further, See discloses that keys are exchanged during the mutual authentication process between the client device/authentication agent and central authentication server/authentication server 320 (col. 5, lines 38-47). When authenticating the other entity, the other's entity must be determined to establish mutual trust.
4. Applicant's response (p. 20) argues that See does not suggest "authenticating said second electronic device to said first electronic device, said first electronic device communicatively coupled to said second electronic device, said second electronic device an authentication server". However, as disclosed in col. 5, lines 38-47, See discloses authenticating an authentication server to a first electronic device/agent.

Art Unit: 2134

5. Applicant's response (p. 21) argues that See does not teach, "determining a key at said first electronic device and at said second electronic device." However, See discloses that keys are exchanged. Therefore, from the viewpoint of either entity, one's own key must be determined for exchange and the received key must be determined to be the expected key. Therefore, a key is determined.

6. Applicant's response (p. 21) argues that See does not describe an edge device as an end system. However, the limitation "end system" is not recited in the claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Further, as the agent is acting on behalf of the client and the system of See can include one edge device per end user, it is maintained that the edge device is a client device from the viewpoint of the user. Additionally, in the well-known client-server model of computing, the edge server in the See reference is a client to the authentication server.

7. Applicant's response (p. 22) argues that because Schneier recites "Here's a protocol that will not work", anything combined with Schneier in such a manner is inoperable. However, Schneier in fact discloses that the interlock protocol accomplishes mutual authentication. However, Schneier discloses that under some circumstances, an intruder can launch a man-in-the-middle attack (p. 55). This statement is therefore understood in such a way that, while the interlock protocol does accomplish mutual authentication, it *can* be the subject of attacks. However, all cryptographic protocols are subject to attacks. In the absence of an attacker with the necessary resources to launch such an attack, the interlock protocol performs its function.

Art Unit: 2134

8. Applicant's response (p. 23) argues that Aboba does not remedy the shortcomings of See. However, as shown above, it is maintained that See discloses the allegedly missing claimed limitations.

9. Applicant's response (p. 24) argues that substantial modifications to the network of See would be necessary to combine the teachings of Derfler with the teaching of See because See describes a wired network. However, the benefits of wireless network configurations are well known in the art of networking, as well as the conversion of wired to wireless, as evidenced by Derfler. Further, it is maintained that the OSI model of networking abstracts the details so that at the application level, the underlying structure of the communications is not known and as such known modifications to the physical layer of See's invention would require little or no modification to the implemented inventive concept. Therefore, using a wireless LAN to couple the first and second devices would only require knowledge well within the realm of one having ordinary skill in the art.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. Claims 1, 8-9, 19, 21, 28-29, 39, 41, 48-49 & 59 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,070,243 to See et al. (See).

Regarding claims 1, 19, 21, 39, 41 & 59, See discloses in a network comprising a first electronic device/intelligent edge device (Fig. 1, #10) and a second electronic device/network management station (Fig. 1, #20), said second device an authentication server (Fig. 3A), an authentication method comprising authenticating said second electronic device/network management station to said first electronic device/intelligent edge device (col. 5, lines 43-47), said first electronic device a client device (col. 5, lines 43-47), said first electronic device communicatively coupled to said second electronic device (Fig. 1), authenticating said first electronic device to said second electronic device (col. 5, lines 43-47), determining a key at said first electronic device and at said second electronic device (col. 5, lines 45-47) and authenticating a user to a central authentication server (col. 5, lines 59-62, col. 6, lines 4-18 & col. 8, lines 14-48).

Regarding claims 8, 28 & 48, See discloses a method, wherein the first electronic device is a client device/intelligent edge device (Fig. 1, #10) and said second electronic device/network management station (Fig. 1, #20) is a central authentication server (Fig. 3A, #320).

Regarding claims 9, 29 & 49, See discloses a method, wherein a network device/intelligent edge device (Fig. 3A) is employed for providing an interface/ID RLY between said client device/intelligent edge (ID REQ) device and said central authentication server (Fig. 1).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2134

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

13. Claims 10-11, 30-31 & 50-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over See, as applied to claims 9, 29 & 49 above, in view of Applied Cryptography, Second Edition by Schneier, in further view of Computer Dictionary, Third Edition by Microsoft. See lacks receiving a first standard message from said client device and receiving said first standard message at said central authentication server whereby said client device is identified to said central authentication server. However, Schneier teaches a simple mutual authentication protocol, where Alice encrypts shared data with Bob's public key and sends it to him to verify Alice's authenticity (p. 54, §Mutual Authentication Using the Interlock Protocol, (1) and (5)) and Bob does the same in reverse (p. 54, §Mutual Authentication Using the Interlock Protocol, (3) and (4)). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify See to use the Interlock protocol, and hence to send a first standard message from the client device to the central authentication server to identify the client to the server and to send a second standard message from the central authentication server to the client to identify the server to the client. One of ordinary skill in the art would have been motivated to perform such a modification to permit the client and authentication server to mutually authenticate each other, as taught by Schneier (p. 54, §Mutual Authentication Using the Interlock Protocol, (1)-(5)). As modified, See lacks explicitly receiving the first standard message at said network device and forwarding the message to the central authentication server and receiving a second standard message from the central authentication server and forwarding it to the client. However, Microsoft teaches that a router is an intermediary device on a

Art Unit: 2134

communications network that expedites message delivery and links many computers together by receiving transmitted messages and forwarding them to their correct destinations (p. 415, §Router). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify See to include a network device/router between the client/intelligent edge device and the central authentication server, and hence to receive the first standard message from the client and forward the message to the authentication server and to receive a second standard message from the authentication server and forward the message to the client. One of ordinary skill in the art would have been motivated to perform such a modification to expedite message delivery and link many computers together, as taught by Microsoft (p. 415, §Router).

14. Claims 10-17, 30-37 & 50-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over See, as applied to claims 9, 29 & 49 above, in view of "PPP EAP TLS Authentication Protocol" by Aboba et al. (**Aboba**).

Regarding claims 10, 13, 30, 33, 50 & 53, as described above, See lacks receiving a first standard message from said client device and receiving said first standard message at said central authentication server whereby said client device is identified to said central authentication server. However, Aboba teaches the EAP TLS protocol to permit mutual authentication and key exchange between two endpoints (p. 1, §1, ¶2). The protocol includes receiving a first standard message/client response packet (p. 4, ¶3) from the client to the authenticator (p. 2, §3.1) at a network device/authenticator acting as a passthrough (p. 2, §3.1) and forwarding said first standard message/client response packet to a central authentication server/RADIUS server or

Art Unit: 2134

backend security server (p. 2, §3.1 & p. 4, ¶3) and receiving said first standard message/client response packet at said central authentication server/RADIUS/EAP server, whereby the client device is identified to said central authentication server (p. 4, ¶4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to receive a first message from a client at a network device and forward the message from the network device to a central authentication server. One of ordinary skill in the art would have been motivated to perform such a modification to permit mutual authentication and key exchange between two endpoints, as taught by Aboba (p. 1 §1 ¶2, p. 2 §3.1 & p. 4 ¶3-4).

Regarding claims 11, 14-15, 31, 34-35, 51 & 54-55, See lacks sending a second standard message to the network device from said central authentication server and forwarding the message to the client from the network device. However, Aboba teaches the EAP TLS protocol to permit mutual authentication and key exchange between two endpoints (p. 1, §1, ¶2). The protocol includes sending a second standard message/server key exchange message (p. 4, ¶1) to the network device/authenticator acting as a passthrough (p. 2, §3.1) and forwarding said second standard message to said client, whereby said central authentication server is authenticated to said client device (p. 5, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to send a second message from a central authentication server to a network device and forward the message from the network device to the client. One of ordinary skill in the art would have been motivated to perform such a modification to permit mutual authentication and key exchange between two endpoints, as taught by Aboba (p. 1 §1 ¶2, p. 2 §3.1 & p. 4 ¶3-4).

Regarding claims 12, 16-17, 32, 36-37, 52 & 56-57, See lacks sending a third message to said network device from said client device and forwarding the third message to the central authentication server. However, Aboba teaches the EAP TLS protocol to permit mutual authentication and key exchange between two endpoints (p. 1, §1, ¶2). The protocol includes sending a third message/client key exchange message (p. 4, ¶3-4) to the network device/authenticator acting as a passthrough (p. 2, §3.1) and forwarding the message to the central authentication server/EAP server (p. 4, ¶3-4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to send a third message from the client to a network device and forward the message from the network device to the central authentication server. One of ordinary skill in the art would have been motivated to perform such a modification to permit mutual authentication and key exchange between two endpoints, as taught by Aboba (p. 1 §1 ¶2, p. 2 §3.1 & p. 4 ¶3-4).

15. Claims 18, 38 & 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over See, as applied to claims 1, 21 & 41 above, in view of How Networks Work by Derfler et al. (Derfler). See lacks the first and second devices being communicatively coupled by a wireless connection. However, Derfler teaches that wireless LANs allow users to move around without losing their connection (p. 114). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify See to make use of a wireless LAN to couple the first and second devices. One of ordinary skill in the art would have been motivated to perform such a modification to enable users to move around without losing their connection, as taught by Derfler (p. 114).

Conclusion

16. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. - 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Or faxed to:

(571) 273-8300

Art Unit: 2134

(for formal communications intended for entry)

Or:

(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS



March 13, 2006

Jaques Bon Jaques
JACQUES H. LOUIS-JACQUES
PRIMARY EXAMINER